UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/562,543	12/28/2005	Thomas Andreas Maria Kevenaar	NL030858	6017

24737 7590 04/17/2009
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
POGMORE, TRAVIS D	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
04/17/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/562,543	KEVENAAR, THOMAS ANDREAS MARIA	
	Examiner	Art Unit	
	Travis Pogmore	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 April 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9 and 12-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9 and 12-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the request for reconsideration filed April 3, 2009.

2. Claims 1-9 and 12-14 are currently pending. Claims 1-9 and 12-14 have been previously presented.

3. Applicant's arguments, with regards to claims 1-9 and 12-14, filed April 3, 2009 have been fully considered but they are not persuasive.

Examiner Notes

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections – 35 USC § 103

5. Claims 1-3, 5-6, 8-9, 12, and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over WIPO Publication No. WO-2000/062503 A2 (hereinafter "Hardjono") in view of European Patent Application Pub. No. EP 1032178 A1 (hereinafter "Chen").

As to claim 1, Hardjono teaches a method of communicating a communication fragment, the communication fragment comprising a first target group address referring to at least two receiver devices (Fig.1 and Fig. 2, e.g. transmitting to a multicast group as depicted in Fig. 1), the method comprising acts of:

a sender device adding a cryptographic message integrity code to protect at least part of the communication fragment, wherein the cryptographic message integrity code

is at least partly based on the target group address (Fig. 2, element 204 and page 7, line 13 to page 8, line 7, the tag (i.e. the cryptographic message integrity code) comprising the base/child encryption key which incorporates the multicast ID number (i.e. target group address)),

the sender device transmitting the protected communication fragment to a router device (Fig. 2, element 206),

Hardjono does not specifically teach the router device, for at least one receiver device in the target group address, replacing the first target group address with an address of the at least one receiver device forming a modified protected communication fragment, while maintaining the unchanged cryptograph message integrity code, and subsequently forwarding the modified protected communication fragment to the at least one receiver device,

the at least one receiver device receiving the modified protected communication fragment,

the at least one receiver device restoring the original protected communication fragment by replacing the address of the at least one receiver device with the target group address to allow verification of the protected communication fragment using the message integrity code.

However, Chen teaches the router device, for at least one receiver device in the target group address, replacing the first target group address with an address of the at least one receiver device forming a modified protected communication fragment, while maintaining the unchanged cryptograph message integrity code, and subsequently

forwarding the modified protected communication fragment to the at least one receiver device (column 10, lines 7-21 and column 11, line 58 through column 12, line 12, the home agent acts as the router device and suggests that it may be necessary to amend any error checking while not mandating that the home agent does so, and the foreign agent acts as a receiver device),

the at least one receiver device receiving the modified protected communication fragment (column 12, lines 2-12),

the at least one receiver device restoring the original protected communication fragment by replacing the address of the at least one receiver device with the target group address to allow verification of the protected communication fragment using the message integrity code (column 12, lines 2-12, the home address being equivalent to the group address).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the teaching of Hardjono to include the router device directly modifying the target address reference and the receiver device restoring the original protected communication of Chen because this would avoid longer communication fragments normally needed (Chen, column 3, lines 25-34).

As to claim 2, Hardjono and Chen do not specifically teach wherein the first communication fragment comprises a bit field IA to indicate whether indirect addressing is used.

However, the concept and advantages of using a bit field to indicate whether an indirect address is being used is well known and expected in the art. For example U.S. Patent App. Pub. No. US 2003/0223402 A1 (page 2, paragraph 30, multicast by its nature uses indirect addressing).

Therefore it would have been obvious to a person having ordinary skill in the art at the time of the invention was made to modify the teaching of Hardjono and Chen to use a single bit to indicate whether or not indirect addressing was being used.

As to claim 3, Hardjono teaches wherein the sender device and the at least one receiver device share a common cryptographic key, and where the cryptographic message integrity code is computable and verifiable only by using the common cryptographic key (page 6, lines 12-13 and 19-20), but does not specifically teach wherein the common cryptographic key is not shared with the router.

However, wherein the common cryptographic key is not shared with the router is well known and expected in the art (e.g. US Patent Application Pub. No. US 2002/0078353 A1 (hereinafter "Sandhu"), page 1, paragraph 12 and page 2, paragraph 18, the (possibility of the) presence of an eavesdropper (i.e. the router) being the basis for the use of asymmetric cryptography to avoid the problem of (insecure) symmetric key distribution). Thereby official notice is taken.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Hardjono to use a key unknown by any of the routers since this is well known and expected in the art and allows for the use of an

existing multicast framework (as in Hardjono) to be used for secure communications of different types, e.g. unicast or a different multicast group.

As to claim 5, Hardjono and Chen teach wherein the at least one receiver device restores the protected communication fragment by replacing the address of the at least one receiver device with each of a plurality of group identities (Chen, column 12, lines 4-12) that include the sender device to determine which of the plurality of group identities the message integrity code matches (Hardjono, page 3, lines 17-22).

As to claim 6, Chen teaches wherein

the router device, wherein the act of replacing the first target group address reference, comprises an act of storing the first target address reference in the modified protected communication fragment (column 11, lines 48-57), and

the at least one receiver device restores the protected communication fragment using the stored first target address reference in the modified protected communication fragment in order to allow verification of the message integrity code (column 12, lines 2-12, the restored mobile nodes home address returns the communication fragment/IP packet to it's original state which is what's required for MIC verification).

As to claim 8, Hardjono teaches a router device (page 5, lines 9-10) being arranged to route a communication fragment from a sender device towards a receiver

device, the communication fragment comprising a target group address referring to at least two receiver devices (page 5, lines 10-13), the router device comprising:

receiving means being arranged to receive the communication fragment comprising a cryptographic message integrity code that is at least partly based on the target group address (page 5, lines 10—13 and 16-18 and page 7, line 13 to page 8, line 7, the processing hardware and software recited on line 11 relies on the identification tags (as indicated on page 3, lines 17-22 and comprising the base/child encryption key which incorporates the multicast ID number (i.e. target group address)) to authenticate the messages, so these must be a part of the received and transmitted messages), and

transmitting means being arranged to transmit the modified communication fragment to the one of the at least one two receiver devices (page 9, lines 7-9, routers in Hardjono act as routers, senders and receivers), but does not specifically teach modifying means being arranged to modify the communication fragment, by replacing the target group address by a reference referring to one of the at least two receiver devices, while maintaining the original cryptographic message integrity code without use of a cryptographic key related to the cryptographic message integrity code.

However, Chen teaches modifying means being arranged to modify the communication fragment, by replacing the target group address by a reference referring to one of the at least two receiver devices, while maintaining the original cryptographic message integrity code without use of a cryptographic key related to the cryptographic message integrity code (column 10, lines 7-21 and column 11, line 58 through column

12, line 12, the home agent acts as the modifying means and suggests that it may be necessary to amend any error checking while not mandating that the home agent does so, and the foreign agent acts as a receiver device).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the teaching of Hardjono to include the router device directly modifying the target address reference and the receiver device restoring the original protected communication of Chen because this would avoid longer communication fragments normally needed (Chen, column 3, lines 25-34).

As to claim 9, Hardjono teaches verification means being arranged to verify the cryptographic message integrity code (page 3, lines 13-20, the authenticator reading and authenticating the tags to determine message origin applies equally to MICs),

wherein a target address is a target group address referring to at least two receiver devices (Fig.1 and Fig. 2, e.g. transmitting to a multicast group as depicted in Fig. 1), and

wherein the cryptographic message integrity code is at least partly based on the target address (page 7, line 13 to page 8, line 7, the generated tag (i.e. the cryptographic message integrity code) comprising the base/child encryption key which incorporates the multicast ID number (i.e. target address)).

Hardjono does not specifically teach a receiver device being arranged to receive a modified communication fragment originating from a transmitter device through a

router device, the modified communication fragment being derived from a communication fragment comprising a target address, the receiver device comprising:

receiving means being arranged to receive the modified communication fragment, and

restoring means being arranged to restore the original communication fragment that was used to compute the cryptographic message integrity code included in the modified communication fragment that by replacing an address of the receiver device with the target address.

However, Chen teaches a receiver device being arranged to receive a modified communication fragment originating from a transmitter device through a router device, the modified communication fragment being derived from a communication fragment comprising a target address (column 10, lines 7-21, a care-of address for a single node is a group of at least one receiver device, this is also standard practice for multicast in general), the receiver device comprising:

receiving means being arranged to receive the modified communication fragment (column 12, lines 2-4), and

restoring means being arranged to restore the original communication fragment that was used to compute the cryptographic message integrity code included in the modified communication fragment that by replacing an address of the receiver device with the target address (column 12, lines 4-8).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the teaching of Hardjono to include the

receiver device as in Chen being arranged to receive communication fragments and the means to restore them to their original state used to compute the MIC as in Hardjono, because this would allow care-of and multicast addressing to still utilize an original MIC.

As to claim 12, Hardjono teaches wherein the transmitter device and the receiver device share a common cryptographic key, and where the cryptographic message integrity code is computable and verifiable only by using the common cryptographic key (page 6, lines 12-13 and 19-20), but does not specifically teach wherein the common cryptographic key is not shared with the router.

However, wherein the common cryptographic key is not shared with the router is well known and expected in the art (e.g. Sandhu, page 1, paragraph 12 and page 2, paragraph 18, the (possibility of the) presence of an eavesdropper (i.e. the router) being the basis for the use of asymmetric cryptography to avoid the problem of (insecure) symmetric key distribution). Thereby official notice is taken.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Hardjono to use a key unknown by any of the routers since this is well known and expected in the art and allows for the use of an existing multicast framework (as in Hardjono) to be used for secure communications of different types, e.g. unicast or a different multicast group.

As to claim 14, Hardjono and Chen teach wherein the receiver device is arranged to restore the communication fragment by replacing the address of the receiver device

with each of a plurality of group identities (Chen, column 12, lines 4-12) that include the transmitter device to determine which of the plurality of group identities the cryptographic message integrity code matches (Hardjono, page 3, lines 17-22).

6. Claims 4 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hardjono in view of Chen et al. and further in view of Sandhu.

As to claim 4, Hardjono and Chen et al. do not specifically teach wherein the common cryptographic key is used to encrypt the message content.

However, Sandhu teaches wherein the common cryptographic key is used to encrypt the message content (page 1, paragraphs 9-10).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the teaching of Hardjono in view of Chen et al. to use the common cryptographic key to encrypt the message content of Sandhu, because this would avoid the need to generate, distribute, and store multiple common cryptographic keys to allow both message integrity verification and message encryption.

As to claim 13, Hardjono and Chen et al. do not specifically teach wherein the common cryptographic key is used to encrypt the message content.

However, Sandhu teaches wherein the common cryptographic key is used to encrypt the message content (page 1, paragraphs 9-10).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the teaching of Hardjono in view of Chen et al. to use the common cryptographic key to encrypt the message content of Sandhu, because this would avoid the need to generate, distribute, and store multiple common cryptographic keys to allow both message integrity verification and message encryption.

7. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hardjono.

Hardjono teaches a sender device (page 3, lines 13-17, the "network device") being arranged to transmit a communication fragment through a router device towards a receiver device, the communication fragment comprising a target group address referring to at least two receiver devices (page 3, lines 20-22 and 25-27, the nature of multicasts is such that they include group addresses), the sender device comprising:

protecting means being arranged to add a cryptographic message integrity code to protect at least part of the communication fragment, wherein the cryptographic message integrity code is at least partly based on the target group address and a cryptographic key (page 3, lines 15-17 and page 7, line 13 to page 8, line 7, the generated tag (i.e. the cryptographic message integrity code) comprising the base/child encryption key which incorporates the multicast ID number (i.e. target group address)), and

transmitting means being arranged to transmit the communication fragment to a receiver device through a router device that is not able to modify the cryptographic message integrity code (page 8, line 29 through page 9, line 2, routers in Hardjono act

as routers, senders and receivers and in the embodiment described merely append tags/MICs instead of changing them), but does not specifically teach where the router device does not have access to the cryptographic key.

However, where the router device does not have access to the cryptographic key is well known and expected in the art (e.g. Sandhu, page 1, paragraph 12 and page 2, paragraph 18, the (possibility of the) presence of an eavesdropper (i.e. the router) being the basis for the use of asymmetric cryptography to avoid the problem of (insecure) symmetric key distribution). Thereby official notice is taken.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Hardjono to use a key unknown by any of the routers since this is well known and expected in the art and allows for the use of an existing multicast framework (as in Hardjono) to be used for secure communications of different types, e.g. unicast or a different multicast group.

Response to Arguments

8. Applicant's arguments, see pages 11-12, filed April 3, 2009, with respect to the rejection(s) of claim(s) 8 under 102(b) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Hardjono in view of Chen.

9. Applicant's arguments, with regards to claims 1-7, 9 and 12-14, filed April 3, 2009 have been fully considered but they are not persuasive.

10. On pages 9-10 of the Applicant's Response, Applicant argues that "it is undisputed that Hardjono 'does not specifically teach wherein the cryptographic

message integrity code is at least partly based on the group address' as recited in claim 8 (see, Final Office Action, page 4)."

11. The Examiner wishes to apologize for the misunderstanding caused by the errant phrase, however if the Applicant reads Final Office Action, page 3, it is established in the rejection of claim 8 (as well as elsewhere within the rejections of claims 1, 7 and 9) that Hardjono does, in fact, teach "a cryptographic message integrity code that is at least partly based on the target group address," so clearly it is not undisputed.

12. On pages 10-11 of the Applicant's Response, Applicant argues that "Hardjono does not 'replace the target group address ...' as cited in claim 8," and further that "in Hardjono, the ID numbers of routers do not act as a target group address."

13. This argument has been fully considered and is persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Hardjono in view of Chen (similarly to the rejection of independent claim 1). See the new rejection above.

14. On page 14 of the Applicant's Response, Applicant argues that Hardjono's multicast ID is not a target group address.

15. The Examiner respectfully disagrees with Applicant's argument as Hardjono works with "any conventionally known multicast protocol, such as IP Multicast" (page 5, line 17) which uses target group addresses to distribute packets to interested parties (i.e. members of the multicast target group). These group addresses are "assigned to the multicast that is distributed to and stored in local memory by routers in the multicast" as recited by Hardjono when establishing the properties of the multicast ID and there is

nothing in the sum of Hardjono to suggest the use of multiple means of identifying the multicast group. Lacking such suggestion, as a "multicast ID" and a "target group address" possess the same properties and are used for the same purpose, one would reasonably conclude that they are, in fact, the same.

16. On pages 15-19, of the Applicant's Response, Applicant argues that Chen does not show the feature of "replacing the first target group address with an address of the at least one receiver device" and vice versa.

17. The Examiner respectfully disagrees with Applicant's arguments, because Chen explicitly teaches "replacing the first ... address with an address of the at least one receiver device." The fact that the address is a target group address has already been taught by Hardjono as cited earlier in the rejection of claim 1. This is what the statement "the home address being equivalent to the group address" was and is intended to indicate. Whether Chen operates in a unicast environment or not is irrelevant as that limitation within the claims has already been established by the primary reference.

18. On pages 17-18, of the Applicant's Response, Applicant argues that with regards to claim 7 Hardjono does not teach or suggest routers not having access to cryptographic keys.

19. While, the Examiner agrees that Hardjono does not specifically teach the routers not having access to the cryptographic keys, the Final Office Action has already established that modifying multicast systems in this way to increase security is well known and expected in the art.

20. Therefore, in view of the above reasons, Examiner maintains rejections except as specifically noted above.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Travis Pogmore whose telephone number is (571)270-7313. The examiner can normally be reached on Monday through Thursday between 8:30 a.m. and 4:00 p.m. eastern time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436

/Travis Pogmore/

Examiner, Art Unit 2436